IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Ramarao et al.	Patent Application	
Serial No.:	10/637,172	Group Art Unit:	2135
Filed:	08/07/2003	Examiner: Pich	

For: RPC PORT MAPPER INTEGRITY CHECKER TO IMPROVE SECURITY OF A PROVISIONABLE NETWORK

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-20 stand rejected. Rejections of claims 1-20 are herein appealed.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claim 1 recites a method (100 of Figure 1 and page 8, last full sentence of the specification) for verifying port mapping integrity in a network. The method 100 includes accessing (110 of method 100 of Figure 1 and page 8, last sentence of the specification) port binding information in a port authorization file in the network. The method 100 further includes querying (120 of method 100 of Figure 1 and page 9, first full paragraph) a port mapper for a mapped port assignment. Method 100 further includes comparing (130 of method 100 of Figure 1 and page 9, second full paragraph) the mapped port assignment to the port binding information and initiating (140 of method 100 and page 10, first full paragraph) a response to the comparing.

Independent Claim 8 recites a network port map verification tool in a network comprising a plurality of network port connections. The tool comprises a port assignment file (page 15, first full paragraph) comprising a port authorization in the network; and a port assignment file verifier (page 15, second full paragraph), wherein the verifier is enabled to verify a port assignment against said port authorization (page 15, second full paragraph).

Independent Claim 15 recites a system (200 of Figure 2 and page 11, line one) for protecting network security. The system includes a network server (209

of Figure 2 and page 13, second paragraph) coupled to a network (205 of Figure 2 and page 11, first paragraph), a network client 212 of Figure 2 and page 13, second paragraph) communicatively coupled with the network server via a port (282 of Figure 2 and page 12, first paragraph), a plurality of provisionable services (206 of Figure 2 and page 11, first paragraph) enabled to communicate with the server via a plurality of ports and a port map verification tool (201 of Figure 2 and page 13, last paragraph) enabled to compare a port assignment to a port authorization in the network.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-6, 8-11, 14-18 and 20 stand rejected under 35 U.S.C. 102(a) as being anticipated by Copeland III (us 2002/0144156).

2. Claims 7, 12, and 19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Copeland III (US 2002/0144156) in view of Hrabik (6,988,208).

3. Claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Copeland in view of Nickles (6,134,591).

Arguments

1. Whether Claims 1-6, 8-11, 14-18 and 20 are anticipated by Copeland III (us 2002/0144156).

Appellants respectfully submit that embodiments of the present invention are not anticipated by Copeland III.

Claim 1 recites an embodiment of the present invention directed to (emphasis added):

> A method for verifying port mapping integrity in a network, comprising:
> accessing port binding information in a port authorization file in said network;
> querying a port mapper for a mapped port assignment; comparing said mapped port assignment to said port binding information; and
> initiating a response to said comparing.

Independent Claims 8 and 15 recite similar features. Claims 2-6, that depend from independent Claim 1, Claims 9-11 and 14 that depend from Independent Claim 8, and 16-18 and 20 that depend from Independent Claim 15 also include these features.

MPEP §2131 provides:

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a

> single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). ... "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Appellants respectfully submit that Copeland is very different from the claimed embodiments and fails to anticipate each identical element of Independent Claim 1. Similarly, Appellants submit that Copeland fails to anticipate the identical claimed features of Independent Claims 8 and 15.

Appellants understand Copeland to teach a port profiling engine that "analyzes the flow data to distinguish legitimate flows from probes" (paragraph [0060]. Copeland stores "the most commonly seen network services" for each IP address. Data flows are then compared to "the most commonly seen network services" for each IP address to determine if the traffic is legitimate.

Appellants submit that Copeland fails to anticipate "comparing said mapped port assignment to said port binding information," as claimed. With the present claimed invention, the port binding information is established during initialization of the network (page 9 of the specification) and is not based on observed data flow as with Copeland.

The examiner has indicated that the "port binding information" of the present invention is "information listing which ports are actually being used." This comparison is incorrect. As stated in the specification, the port binding information is established during initialization of the network and includes the permanent bindings which are those ports assigned permanently to particular services or clients (page 9 of the specification). The port binding information is not based on port usage, as with Copeland.

In other words, the port binding information is not directly related to "the ports actually being used" because unauthorized activity may be "using a port" but would not have corresponding port binding information. The present invention compares "the ports actually being used" to the "port binding information" to determine un-authorized port usage.

In the "Response to Arguments" portion of the current Office Action, the Examiner indicates "nowhere in the claim is it required that port binding information be established during initialization of the network. It is recognized that that, although the claims are read in light of the specification, limitations appearing in the specification are not read into the claims.

However, it is also recognized that the claims are read as one of ordinary skill in the art would read them. Furthermore, it is recognized that an Appellant can be his or her own lexicographer, as long as the meaning of a term is not repugnant to the usual meaning of the term. Moreover, if extrinsic reference sources evidence more than one definition for the term, the intrinsic record (e.g., the disclosure of the instant application) must be consulted to identify which of the different possible definitions is most consistent with Appellants' use of the term – where there are several common meanings for a claim term, the patent disclosure serves to point away from the improper meanings and toward the proper meanings.

Appellant respectfully submits the "port binding" words of the claim must be given their plain meaning. In other words, they must be read as they would be interpreted by those of ordinary skill in the art. In re Sneed, 710 F.2d 1544, 218 USPQ 385 (Fed. Cir. 1983). Moreover, the "port binding information" terminology is clearly defined in the Specification and the Figures as being established during initialization of the network and includes the permanent bindings which are those ports assigned permanently to particular services or clients (page 9 of the specification).

In opposition to the "port binding information" of the present invention, the "seen today" list of Copeland is vulnerable to attack. If the "seen today" list of

Copeland is compromised, there is no way of identifying un-authorized port usage. In opposition, with the present invention, if the "mapped port assignment" is compromised, the un-authorized port usage will be identified when the "mapped port assignment" is compared to the port binding information because they will be different. Copeland fails to teach or suggest comparing mapped port assignment to port binding information, as claimed.

For this rational, Copeland does not teach or suggest every element of Independent Claim 1 and similarly, Independent Claims 8 and 15. As such, Appellants believe Claims 1-6, 8-11, 14-18 and 20 are not anticipated by Copeland and respectfully submit the rejection is improper and should be removed.

2. Whether Claims 7, 12, and 19 are patentable over Copeland III (US 2002/0144156) in view of Hrabik (6,988,208).

As stated above, Copeland fails to teach or suggest "comparing said mapped port assignment to said port binding information," as claimed. Appellants submit that Hrabik fails to remedy the deficiencies of Copeland.

In particular, Hrabik fails to teach or suggest "comparing said mapped port assignment to said port binding information," as claimed. Hrabik may teach a

system for testing the integrity of a device on a target network (column 7, lines 16-17), however, Hrabik is silent to "comparing said mapped port assignment to said port binding information," as claimed. Hrabik uses "multiple views" of network activity to determine attacks (column 8, lines 20-40) which is very different from "comparing said mapped port assignment to said port binding information," as claimed.

"As reiterated by the Supreme Court in KSR, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious" (emphasis in original; MPEP 2141.02(I)).

Appellants do not understand the invention as a whole to be obvious in view of Copeland and Hrabik because neither teach or suggest "comparing said mapped port assignment to said port binding information," as claimed.

As such, Claims 7, 12 and 19 are patentable over Copeland in view of Hrabik. Appellants respectfully request the rejection be removed for the rational presented above.

3. Whether Claim 13 is patentable over Copeland in view of Nickles (6,134,591).

As stated above, Copeland fails to teach or suggest "comparing said mapped port assignment to said port binding information," as claimed. Appellants submit that Nickles fails to remedy the deficiencies of Copeland.

Nickles, may teach the use of a digital signature to verify the source of data (column 10, lines 10-38), however, Nickles fails to teach or suggest "comparing said mapped port assignment to said port binding information," as claimed.

Furthermore, Nickles teaches away from the present invention by describing in column 9, lines 25-30 "the random port generator module 88 randomly selects an unused port for which communication." Random selection of port assignment would greatly compound the difficulty of maintaining the "port binding information" of the present invention.

For this rational, Claim 13 is patentable over Copeland in view of Nickles. Appellants respectfully request the rejection be removed.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellant's undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 05/12/2008

/John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNER BLECHER LLP
WESTRIDGE BUSINESS PARK
123 WESTRIDGE DRIVE
WATSONVILLE, CALIFORNIA 95076
408-377-0500

Claims Appendix

1. A method for verifying port mapping integrity in a network, comprising:

accessing port binding information in a port authorization file in said network;

querying a port mapper for a mapped port assignment;

comparing said mapped port assignment to said port binding information; and

initiating a response to said comparing.

2. The method described in Claim 1 wherein said network comprises a utility data center.

3. The method described in Claim 1 wherein said mapped port assignment comprises static port binding data.

4. The method described in Claim 1 wherein said port authorization file comprises fixed port assignments.

5. The method described in Claim 1 wherein said port authorization file is generated upon network initialization.

6. The method described in Claim 1 wherein said response comprises an alarm.

7. The method described in Claim 1 wherein said response comprises a system lockdown.

8. In a network comprising a plurality of network port connections, a network port map verification tool, comprising:

a port assignment file comprising a port authorization in said network; and

a port assignment file verifier, wherein said verifier is enabled to verify a port assignment against said port authorization.

9. The network port map verification tool described in Claim 8 , wherein said network comprises a utility data center.

10. The network port map verification tool described in Claim 9, wherein said network port map verification tool is further enabled to initiate a response to a port assignment anomaly.

11. The network port map verification tool described in Claim 10, wherein said response is an alarm.

12. The network port map verification tool described in Claim 10, wherein said response is a system lockdown.

13. The network port map verification tool described in Claim 9, wherein said network port map verification tool is enabled to verify a digital signature related to said port authorization.

14. The network port map verification tool described in Claim 9, wherein said network port map verification tool is enabled to operate in a remote procedure call environment.

15. A system for protecting network security, comprising:

a network server coupled to a network;

a network client communicatively coupled with said network server via a port;

a plurality of provisionable services enabled to communicate with said server via a plurality of ports; and

a port map verification tool enabled to compare a port assignment to a port authorization in said network.

16. The system for protecting network security described in Claim 15 wherein said network comprises a utility data center.

17. The system for protecting network security described in Claim 15, wherein said port map verification tool is enabled to initiate a response to a port assignment anomaly.

18. The system for protecting network security described in Claim 17, wherein said response can be an alarm.

19. The system for protecting network security described in Claim 17, wherein said response can be a system lockdown.

20. The system for protecting network security described in Claim 17, wherein said port map verification tool is enabled to operate in a remote procedure call environment.

Evidence Appendix

None

Related Proceedings Appendix

None